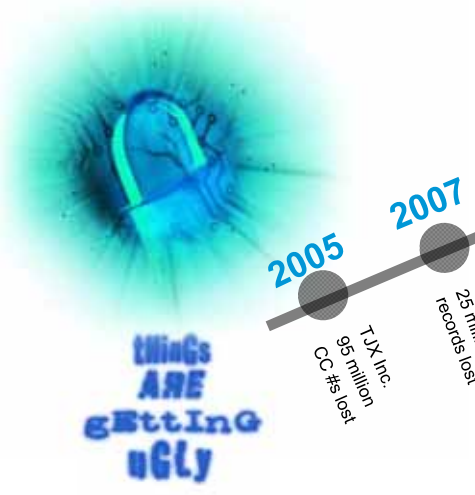
AUS CERT 2012 SECURITY ON THE MOVE

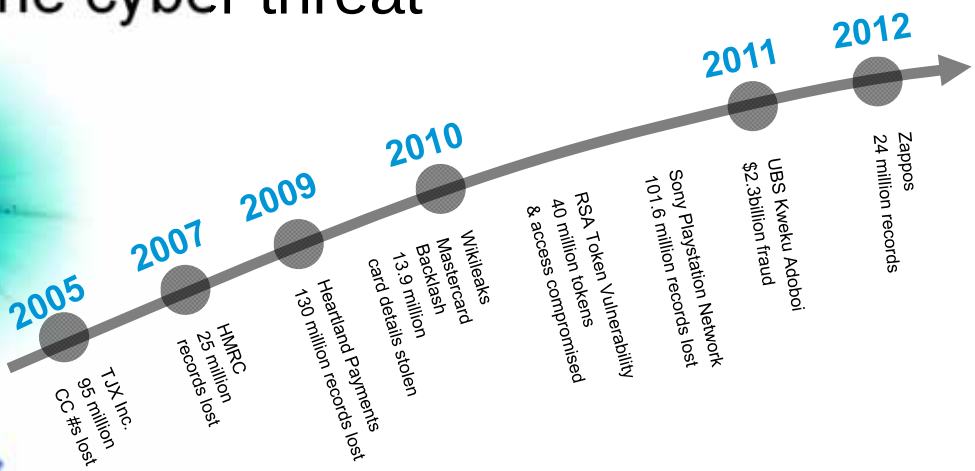
11th Annual AusCERT Information Security Conference 14th - 18th May 2012 AusCERT

The Evolution of Application Monitoring

Narayan Makaram, CISSP,
Director, Solutions Marketing,
HP Enterprise Security Business Unit,
May 18th, 2012

Rise of the cyber threat





Enterprises and Governments are experiencing the most AGGRESSIVE THREAT ENVIRONMENT in the history of information.

Security awareness at board level

Organizational and security leadership is under immense pressure

EXTENDED SUPPLY CHAIN

44% OF DATA BREACH INVOLVED 3RD PARTY MISTAKES

CYBER THREAT

56% ORGANIZATIONS HAVE BEEN THE TARGET OF NATION-STATE CYBER ATTACK

INCREASING COST PRESSURES

11% OF TOTAL IT BUDGET SPENT ON SECURITY

CISO

Chief Information Security Officer sits at heart of the enterprise security response

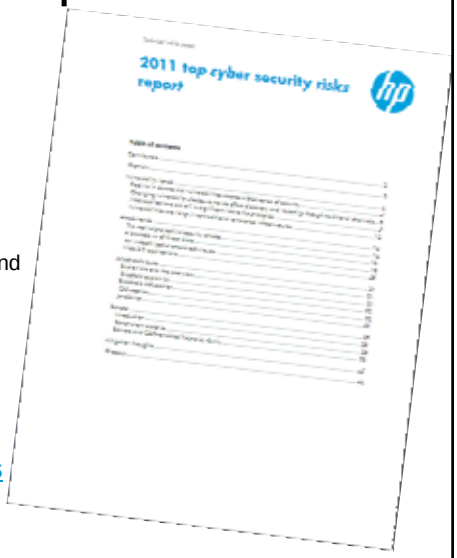
Enterprise security priorities

- Manage **INFORMATION RISK** in the era of mobile, cloud, social media
- Protect against increasingly sophisticated **CYBER THREATS**
- Improve **REACTION TIME** to security incidents
- Reduce costs and **SPEND WISELY**
- Achieve **COMPLIANCE** in a predictable and cost-effective way

Applications: The New Frontier for Cyber Attacks

2011 Top Cyber Security Risks Report

- HP DVLabs biannual report (published since 2009) helps enterprise organizations prioritize security resources
- Uses data from the following sources:
  - Vulnerability information from the Open Source Vulnerability Database (OSVDB) and the HP DVLabs Zero Day Initiative (ZDI)
  - Web application data from the HP Fortify Web Security Research Group and Fortify on Demand
  - Attack information from a worldwide network of HP TippingPoint Intrusion Prevention Systems and a network of honeypots
  - Exploit analysis from HP DVLabs
- Available at http://www.hpenterprisesecurity.com/cybersecurityrisks

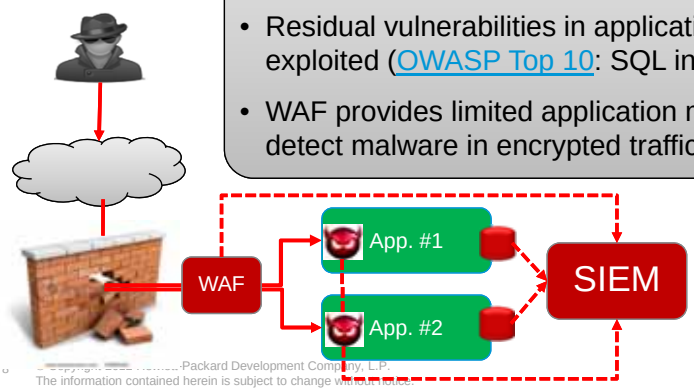


Key Findings

- Regardless of platform (mobile, virtual, etc.), applications are primary target for attack – particularly web applications.
- Vulnerabilities declining in commercial applications but increasing in custom applications.
- Attacks on applications – particularly Web applications – are increasing at an alarming rate.
- New techniques are allowing attackers to use old vulnerabilities to successfully launch new attacks

Application Security Monitoring is easy

- Expensive application re-write required to audit applications (e.g. login sessions, file access, registry updates)
- Longer to develop connectors to forward logs to a central SIEM for security analytics and compliance
- Residual vulnerabilities in applications go undetected and easily exploited (OWASP Top 10: SQL injection, XSS, etc.)
- WAF provides limited application monitoring, more overhead, and cannot detect malware in encrypted traffic (SSL)



Best Practices for Application Security
Why are they NOT working?

- Adopt secure software development life cycle (SDLC)
  - Slow Adoption: It takes years to train developers/testers to build in security
  - 3rd Party Code: Cannot impose SDLC practices on 3rd parties and SAAS providers
- Detect application vulnerabilities during staging before production
  - Developers accustomed to logging functional use-cases not abuse-cases
  - Businesses under pressure to on-board web-applications before running penetration tests
- Detect and Protect against application threats during operations
  - Cannot detect and protect against application attacks without runtime context
  - Need session and activity logs to detect abnormal user activity in applications
  - Need SIEM to correlate across multiple event sources to identify business risk

HP Security Strategy

HP Enterprise Security

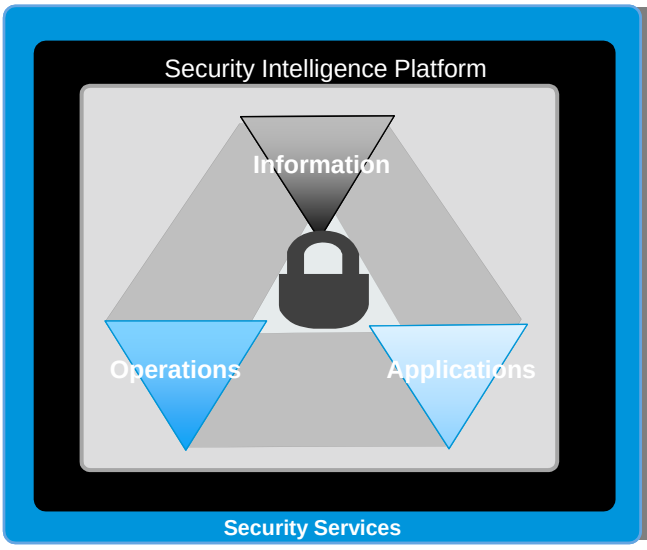
Market leading products and services

- Security Information and Event Management
- Log Management
- Application Security
- Network Security
- Data Protection
- Threat Research
- Security Services

One Team, One Vision

DVLabs
TippingPoint
ATALLA
ArcSight
VISTORM
FORTIFY
SPI DYNAMICS

HP Security Intelligence Platform



Establish complete **visibility** across all applications and systems

Analyze vulnerabilities in applications and operations to understand risk

Respond adaptively to build defenses against the exploitation of vulnerabilities

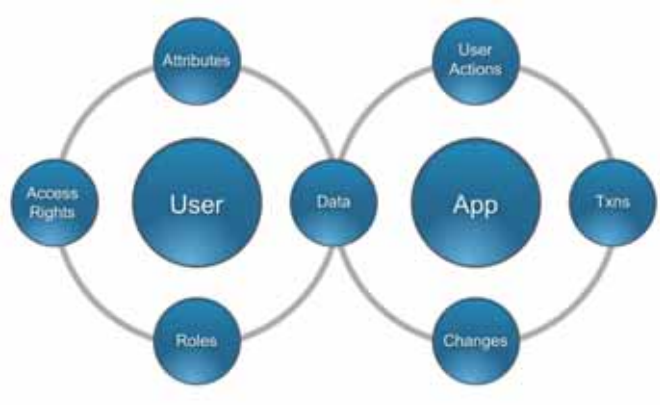
Measure security effectiveness and risk across people, process, and technology to improve over time

Increased Situational Awareness

Provide Context

Traditional Security Monitoring

Hybrid Security Monitoring



Security Intelligence and Risk Management Solutions

HP ESP Professional Services

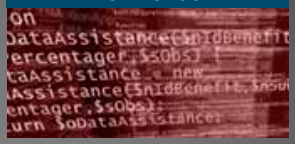
UNIVERSAL LOG MANAGEMENT

Effectively manage risk and compliance at business-process level

COMPLIANCE & RISK MANAGEMENT

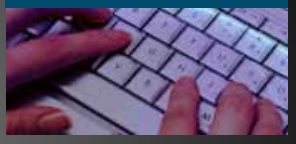
Leverage centralized logging to maintain SOX, PCI, FISMA and HIPAA compliance

PERIMETER & NETWORK SECURITY



Adaptive monitoring to maintain network integrity and availability with superior network transparency

INSIDER THREAT



Detect threats from within by correlating users with roles and activity

ADVANCED PERSISTENT THREAT

Identify anomalous behavior with grater insight into network and users

SOFTWARE SECURITY ASSURANCE

Achieve Security-by-default software development capabilities

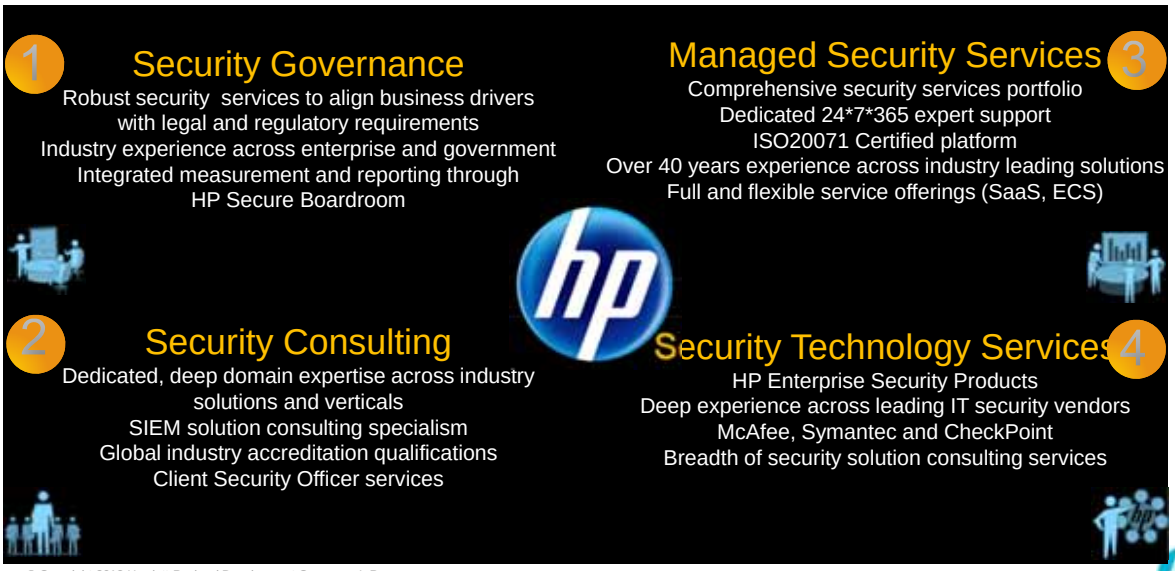
DATA PRIVACY & DATA LOSS MONITORING

Proactively detect and mitigate security and privacy breaches

APPLICATION & TRANSACTION MONITORING

Track application activity for signs of fraud and abuse

HP Enterprise Security Services

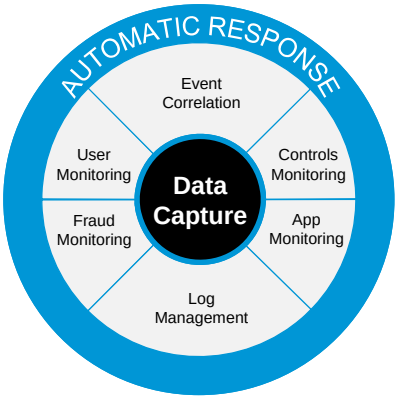


15

HP Application Security Solutions

HP ArcSight SIEM Solution

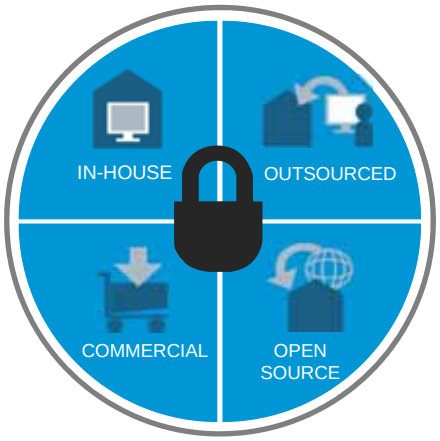
A comprehensive platform for monitoring modern threats and risks, augmented by services expertise and the most advanced security user community, Protect724



- **Establish** complete visibility
- **Analyze** events in real time to deliver insight
- **Respond** quickly to prevent loss
- **Measure** security effectiveness across people, process and technology

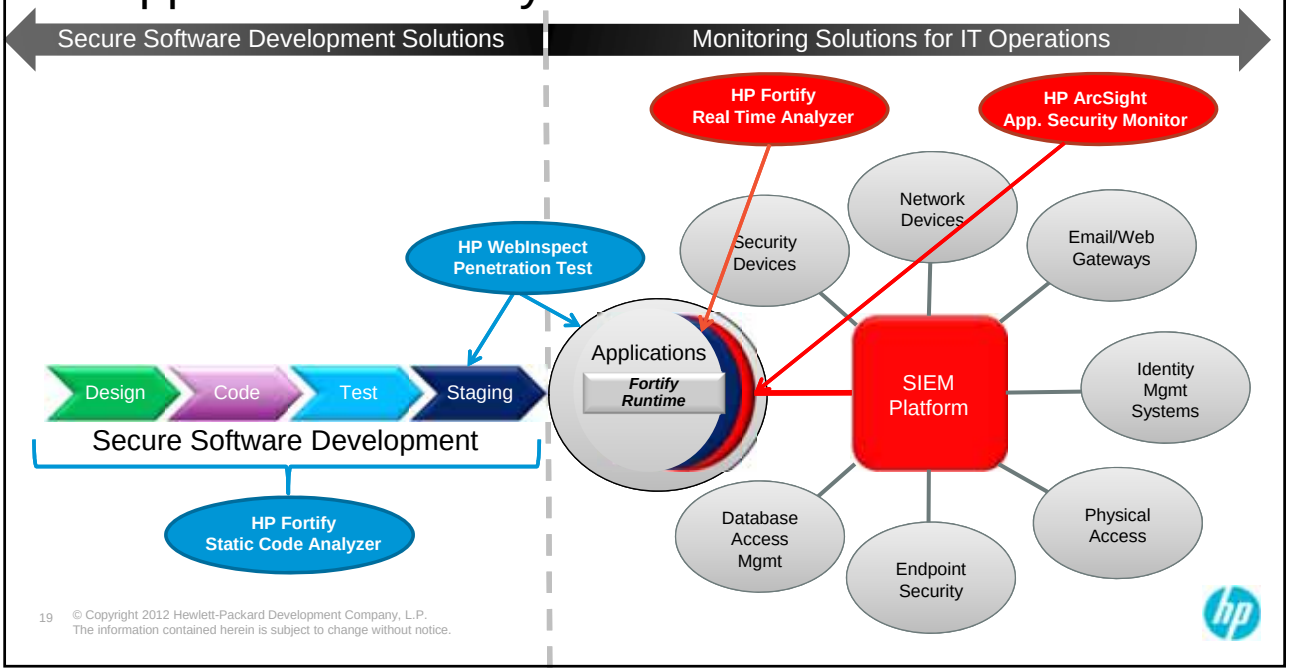
HP Fortify Application Security Solutions

Identifies and eliminates risk in existing applications and prevents the introduction of risk during application development, in-house or from vendors.

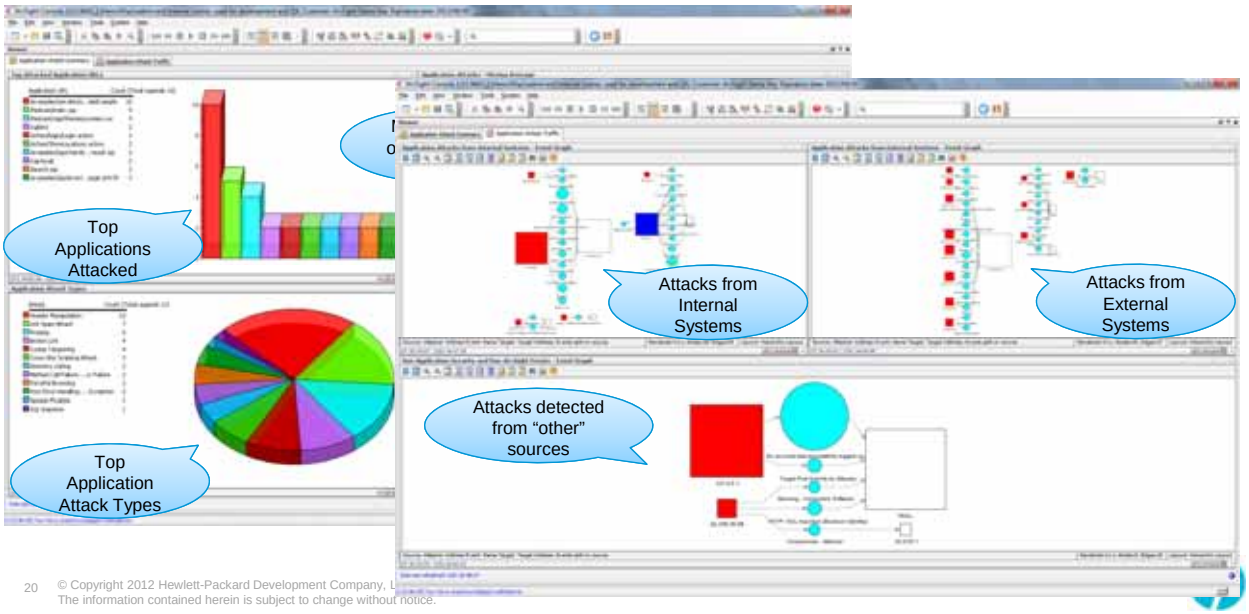


- **Protects** business critical applications from advanced cyber attacks by removing security vulnerabilities from software
- **Accelerates** time-to-value for achieving secure applications
- **Increases** development productivity by enabling security to be built into software, rather than added on after it is deployed
- **Delivers** risk intelligence from application development to improve operational security

HP Application Security Solutions

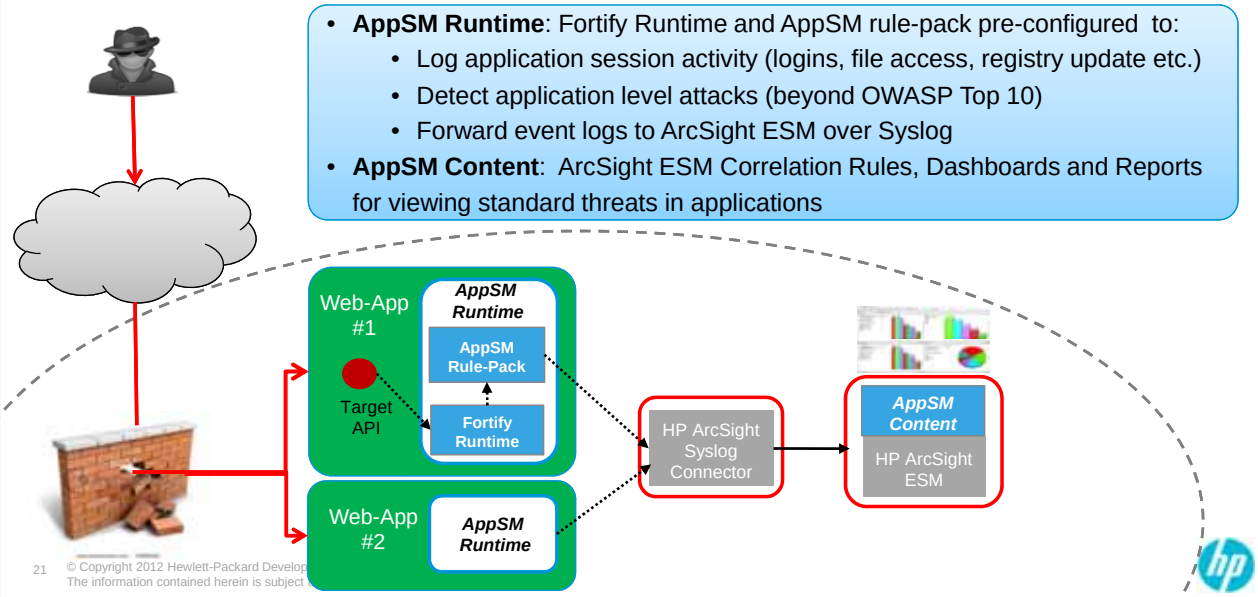


HP ArcSight AppSM Dashboard



HP ArcSight Application Security Monitor (AppSM)

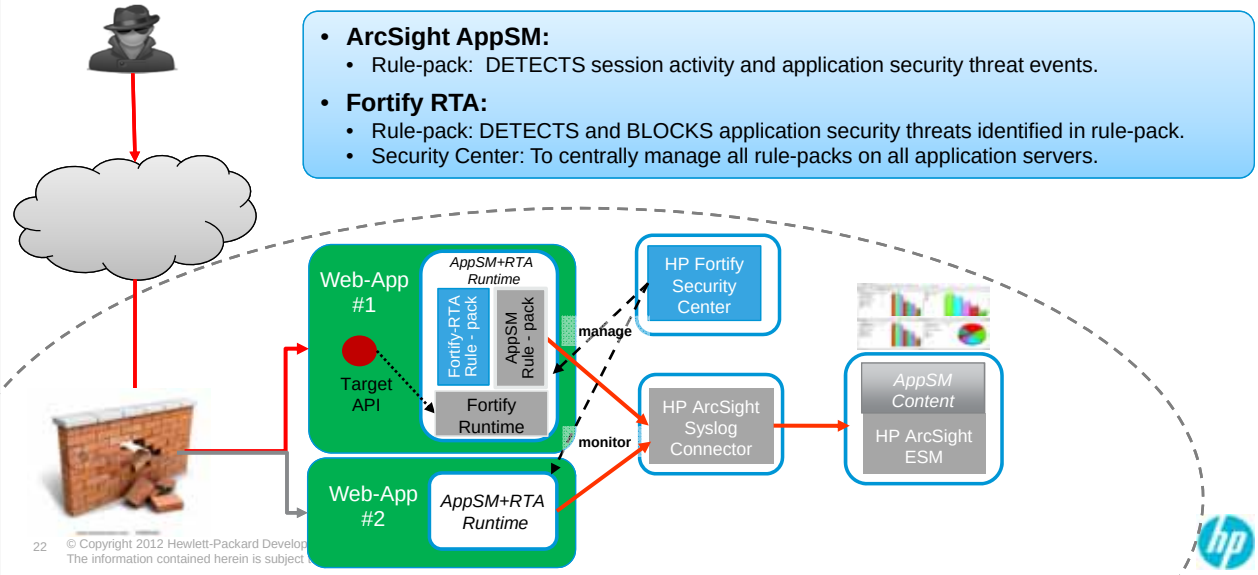
- **AppSM Runtime**: Fortify Runtime and AppSM rule-pack pre-configured to:
  - Log application session activity (logins, file access, registry update etc.)
  - Detect application level attacks (beyond OWASP Top 10)
  - Forward event logs to ArcSight ESM over Syslog
- **AppSM Content**: ArcSight ESM Correlation Rules, Dashboards and Reports for viewing standard threats in applications



HP Fortify Run Time Analyzer (RTA)

Adds Application Threat Protection and Centralized Management

- **ArcSight AppSM:**
  - Rule-pack: DETECTS session activity and application security threat events.
- **Fortify RTA:**
  - Rule-pack: DETECTS and BLOCKS application security threats identified in rule-pack.
  - Security Center: To centrally manage all rule-packs on all application servers.



Summary

- Adopt secure software development life cycle (SDLC)
  - Train software developers/testers to build in security during SDLC
  - Use tools to identify security risks early during software development
- Detect application vulnerabilities during staging before production
  - Run penetration testing tools that detect residual vulnerabilities in applications
- Detect and Protect against application threats during operations
  - Use tools that allow you to rapidly detect and protect application level threats without modifying applications
  - Address critical application level threats by correlating application events with events reported by other enterprise sources using SIEM

Find out more

HP Enterprise Security Products

- Gab Gennai
- +61 411 606 050
- Gabriel.gennai@hp.com

- Shlomi Shaki
- +61 407 225 944
- Shlomi Shaki@hp.com

- Stephen MacDonald
- +61 423 776 606
- Stephen.macdonald@hp.com

HP Enterprise Security Services

- Rob Hueston
- +61 407 163 088
- Rob.hueston@hp.com

- Jeremy Roach
- +61 423 781 190
- Jeremy.roach@hp.com

- Andrew Latham
- +61 406 537 576
- alatham@hp.com

After the event

- Contact your sales rep
- Visit us at: http://www.hpenterprisesecurity.com

Thank You